AVG Email Server Edition 2013

Manual del usuario

Revisión del documento 2013.02 (03/12/2013)

Contenido

1. Introducción

Este manual del usuario proporciona documentación completa sobre **AVG Email Server Edition 2013**.

Enhorabuena por adquirir AVG Email Server Edition 2013.

AVG Email Server Edition 2013 es un software de la gama de productos galardonados de AVG que están diseñados para darle tranquilidad a usted y total seguridad a su servidor. Al igual que el resto de productos AVG, **AVG Email Server Edition 2013** se ha rediseñado íntegramente, de arriba a abajo, para proporcionar la reconocida y acreditada protección de seguridad de AVG de forma novedosa, más eficiente y fácil de usar.

AVG ha sido diseñado y desarrollado para proteger su actividad informática y de red. Disfrute la experiencia de una protección total con AVG.

Nota: *esta documentación contiene una descripción de las características específicas de Email Server Edition. Para obtener información acerca de otras características de AVG, consulte la guía del usuario de Internet Security Edition, que contiene todos los detalles necesarios. Puede descargar la guía desde http://www.avg.com.*

2. Requisitos de instalación de AVG

2.1. Sistemas operativos compatibles

AVG Email Server Edition 2013 se ha diseñado para proteger los servidores de correo electrónico con los siguientes sistemas operativos:

- Windows 2012 Server Edition (x86 y x64)
- Windows 2008 Server Edition (x86 y x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Servidores de correo electrónico compatibles

Son compatibles los siguientes servidores de correo:

- MS Exchange 2003 Server
- MS Exchange 2007 Server
- MS Exchange 2010 Server
- MS Exchange 2013 Server
- Kerio MailServer: versión 6.7.2 y superior

2.3. Requisitos de hardware

Requisitos de hardware mínimos para **AVG Email Server Edition 2013**:

- CPU Intel Pentium de 1,5 GHz
- 500 MB de espacio libre en disco duro (para la instalación)
- 512 MB de memoria RAM

Requisitos de hardware recomendados para **AVG Email Server Edition 2013**:

- CPU Intel Pentium de 1,8 GHz
- 600 MB de espacio libre en disco duro (para la instalación)
- 512 MB de memoria RAM

2.4. Desinstalar versiones anteriores

Si tiene instalada una versión más antigua de AVG Email Server, necesitará desinstalarla de forma manual antes de instalar **AVG Email Server Edition 2013**. Debe realizar de forma manual la desinstalación de la versión anterior, utilizando la funcionalidad estándar de Windows.

- Desde el menú de inicio ***Inicio/Configuración/Panel de control/Agregar o quitar programas***, seleccione el programa correcto de la lista de software instalado. También puede desinstalarla, y quizás con mayor facilidad, a través del menú ***Inicio/Todos los programas/AVG/Uninstall AVG***.

- Si ha utilizado anteriormente la versión AVG 8.x o anterior, no olvide desinstalar también los complementos individuales del servidor.

  Nota: *será necesario reinstalar el servicio de almacenamiento durante el proceso de desinstalación.*

  Complemento de Exchange: ejecute setupes.exe con el parámetro /uninstall desde la carpeta en la que se instaló el complemento:

  p. ej., C:\AVG4ES2K\setupes.exe /uninstall

  Complemento de Lotus Domino/Notes: ejecute setupln.exe con el parámetro /uninstall desde la carpeta en la que se instaló el complemento:

  p. ej., C:\AVG4LN\setupln.exe /uninstall

2.5. Service Packs de MS Exchange

No es necesario ningún Service Pack para MS Exchange 2003 Server; sin embargo, se recomienda mantener el sistema actualizado con los Service Packs y revisiones más recientes para obtener la máxima seguridad disponible.

Service Pack para MS Exchange 2003 Server (opcional):

http://www.microsoft.com/en-us/download/details.aspx?id=9664

Al comienzo de la instalación, se examinarán todas las versiones de las bibliotecas del sistema. Si resulta necesario instalar bibliotecas nuevas, el instalador añadirá a la extensión .delete al nombre de las antiguas. Se eliminarán al reiniciar el sistema.

Service Pack para MS Exchange 2007 Server (opcional):

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

Service Pack para MS Exchange 2010 Server (opcional):

http://www.microsoft.com/en-us/download/details.aspx?id=28190

3. Proceso de instalación de AVG

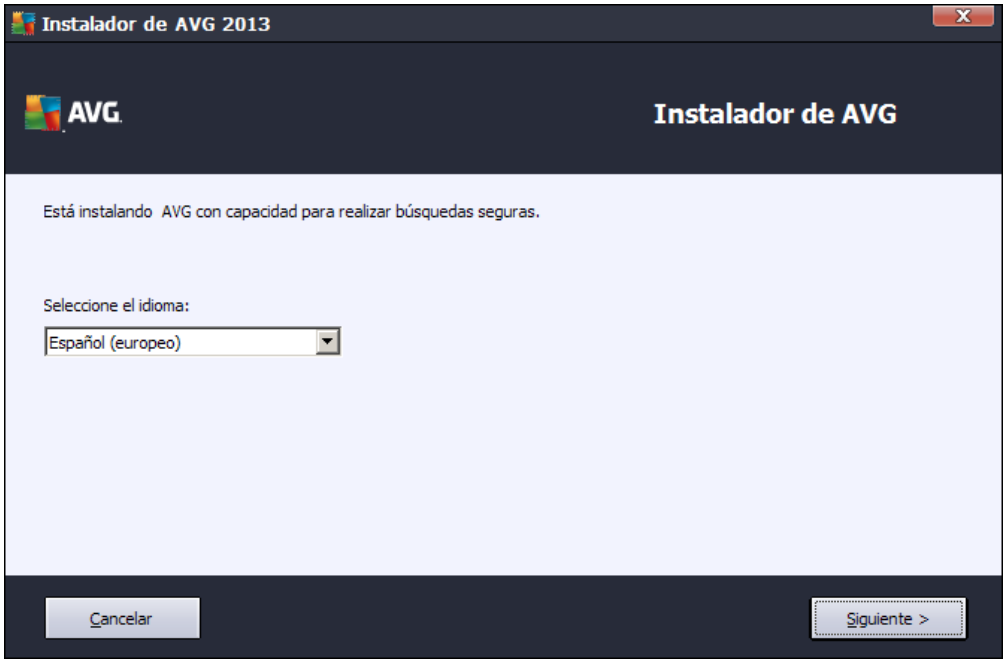
Para instalar AVG en su equipo, debe obtener el archivo de instalación más reciente. Puede utilizar el archivo de instalación del CD que forma parte de la edición en caja, aunque este archivo podría estar obsoleto. Por este motivo, se recomienda obtener en línea el archivo de instalación más reciente. Puede descargar el archivo del sitio web de AVG (en http://www.avg.com/download?prd=msw).

Hay dos paquetes de instalación disponibles para su producto: para sistemas operativos de 32 bits (señalados como x86) y para sistemas operativos de 64 bits (señalados como x64). Asegúrese de utilizar el paquete de instalación adecuado para su sistema operativo específico.

Durante el proceso de instalación se le solicitará el número de licencia. Asegúrese de tenerlo a mano antes de comenzar la instalación. El número figura en el paquete del CD. Si compró su copia de AVG en línea, el número de licencia se le habrá enviado por correo electrónico.

Una vez que haya descargado y guardado el archivo de instalación en el disco duro, puede iniciar el proceso de instalación. La instalación es una secuencia de ventanas de cuadro de diálogo con una breve descripción de lo que se debe hacer en cada paso. A continuación ofrecemos una explicación de cada ventana de cuadro de diálogo:

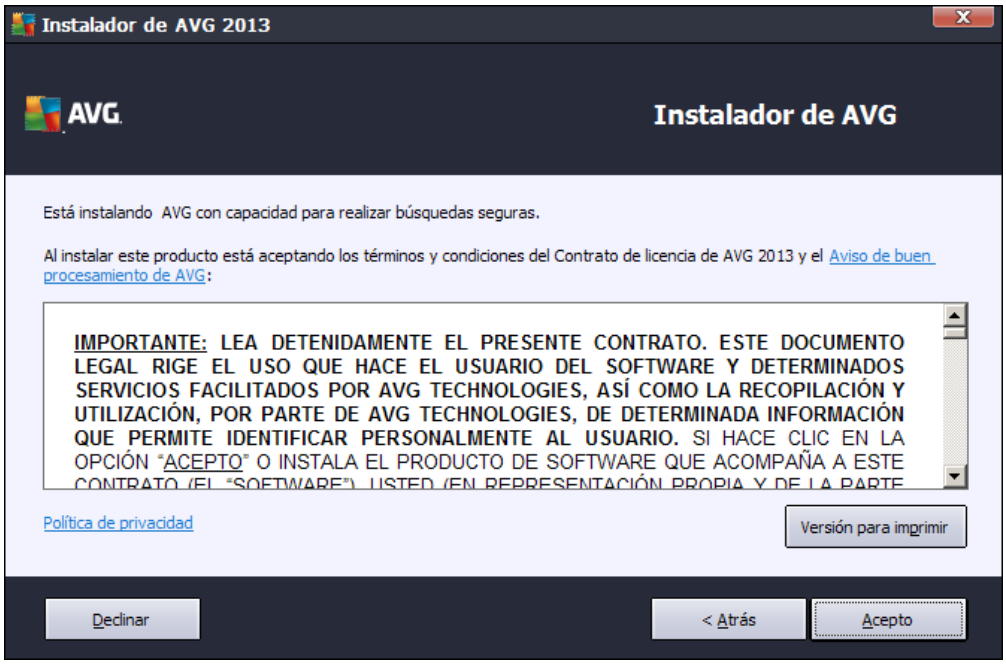
3.1. Inicio de la instalación



El proceso de instalación se inicia con la ventana de cuadro de diálogo de bienvenida. En ella, seleccione el idioma usado para el proceso de instalación y pulse el botón ***Siguiente***.

Podrá elegir más idiomas para la interfaz de la aplicación posteriormente durante el proceso de instalación.

3.2. Contrato de licencia

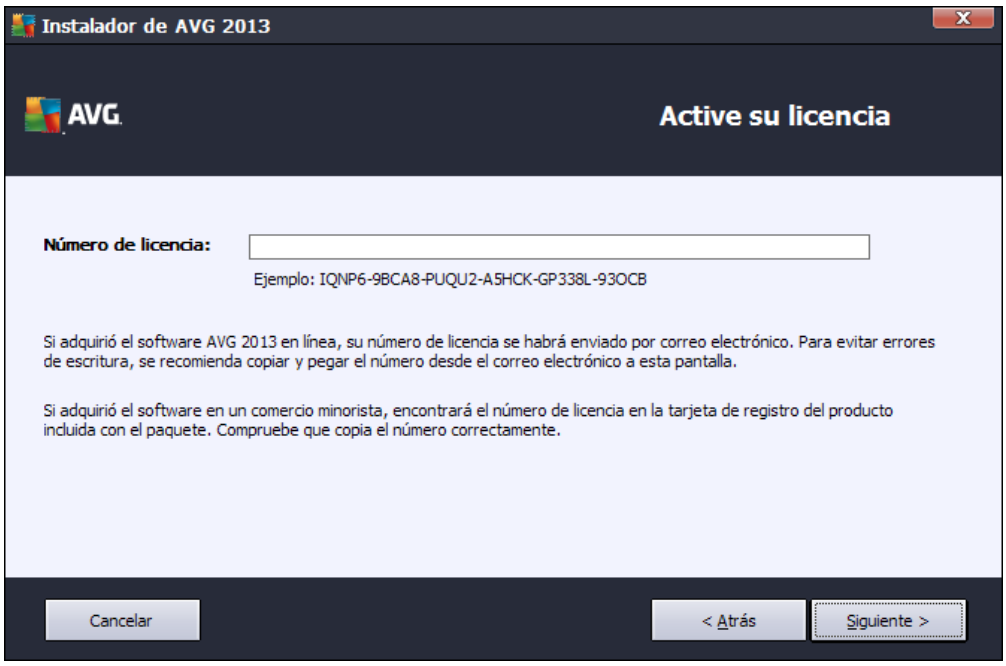


Este cuadro de diálogo le permite leer las condiciones de la licencia. Utilice el botón ***Versión para imprimir*** para abrir el texto de la licencia en una nueva ventana. Pulse el botón ***Acepto*** para confirmar y pasar al cuadro de diálogo siguiente.

3.3. Active su licencia

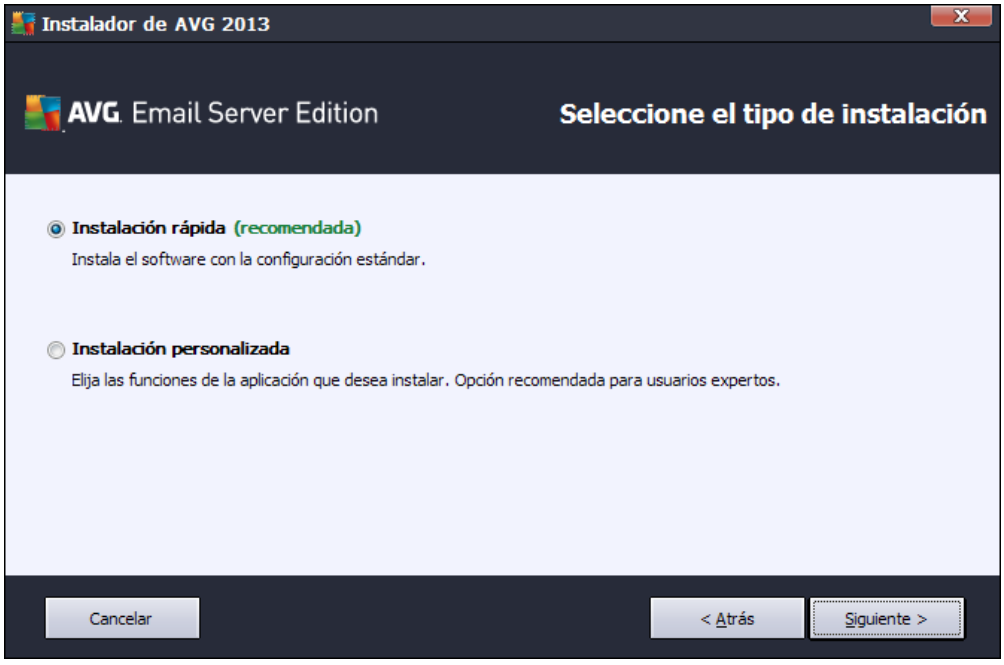
En el cuadro de diálogo ***Active su licencia*** debe introducir su número de licencia.

Escríbalo en el campo de texto ***Número de licencia***. El número de licencia se encontrará en el correo electrónico de confirmación que recibió después de haber comprado AVG en línea. Debe introducir el número tal como figura. Si cuenta con el formato digital del número de licencia (en el correo electrónico), se recomienda usar el método copiar y pegar para insertarlo.



Pulse el botón ***Siguiente*** para continuar con el proceso de instalación.

3.4. Seleccione el tipo de instalación



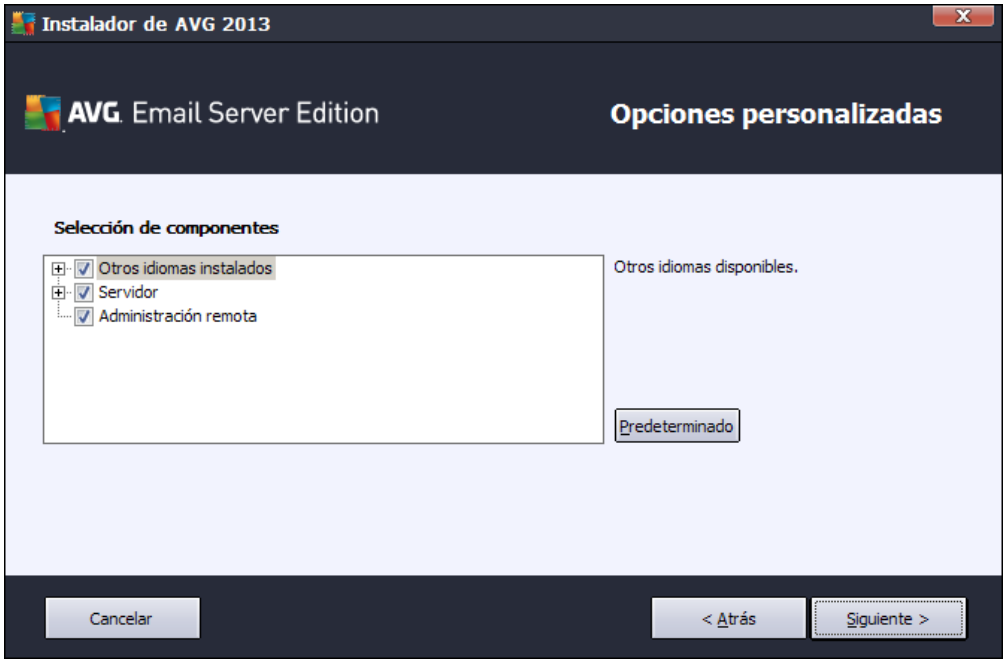
El cuadro de diálogo ***Seleccione el tipo de instalación*** permite elegir entre dos opciones de instalación: ***Instalación rápida*** e ***Instalación personalizada***.

Para la mayoría de los usuarios, se recomienda seleccionar la opción ***Instalación rápida***, que instala AVG de manera totalmente automática con la configuración predefinida por el proveedor del programa. Esta configuración ofrece máxima seguridad con un uso óptimo de los recursos. En el futuro, si fuese necesario modificar la configuración, siempre tendrá la posibilidad de hacerlo directamente desde la aplicación AVG.

La ***Instalación personalizada*** solo debería ser utilizada por usuarios expertos que tengan una razón válida para instalar AVG con una configuración diferente de la estándar. Por ejemplo, para adecuar el programa a necesidades específicas del sistema.

Al seleccionar Instalación personalizada, la sección ***Carpeta de destino*** aparece en la parte inferior del cuadro de diálogo. Permite especificar la ubicación en la que debe instalarse AVG. De manera predeterminada, AVG se instalará en la carpeta de archivos de programa situada en la unidad C:. Si desea cambiar esta ubicación, utilice el botón ***Examinar*** para mostrar la estructura de la unidad y seleccione la carpeta en cuestión.

3.5. Instalación personalizada - Opciones personalizadas



La sección ***Selección de componentes*** muestra una descripción general de todos los componentes de AVG que se pueden instalar. Si la configuración predeterminada no se ajusta a sus necesidades, puede quitar o agregar componentes específicos.

Sin embargo, solamente puede seleccionar componentes incluidos en la edición de AVG que haya adquirido. Solo se ofrecerá la posibilidad de instalar estos componentes específicos en el cuadro de diálogo Selección de componentes.

- ***Administración remota***: si planea conectar AVG a un Centro de datos de AVG (AVG Network Edition), tendrá que seleccionar esta opción.

- ***Otros idiomas instalados***: puede especificar en qué idiomas deberá instalarse AVG. Marque el elemento ***Otros idiomas instalados*** y luego seleccione los idiomas deseados del menú correspondiente.

Información general básica de los componentes individuales del servidor (en la rama ***Servidor***):

- ***Servidor anti-spam para MS Exchange***

  Comprueba todos los mensajes de correo electrónico entrantes y marca el correo no deseado como SPAM. Utiliza varios métodos de análisis para procesar cada mensaje, además de ofrecer la máxima protección posible contra el correo no deseado.

- ***Analizador de correo electrónico para MS Exchange (agente de transporte enrutador)***

  Comprueba todos los mensajes de correo electrónico entrantes, salientes e internos que van a través de la función HUB de MS Exchange.

- ***Analizador de correo electrónico para MS Exchange (agente de transporte SMTP)***

  Comprueba todos los mensajes de correo electrónico que llegan a través de la interfaz SMTP de MS Exchange (se puede instalar para las funciones EDGE y HUB).

- ***Analizador de correo electrónico para MS Exchange (VSAPI)***

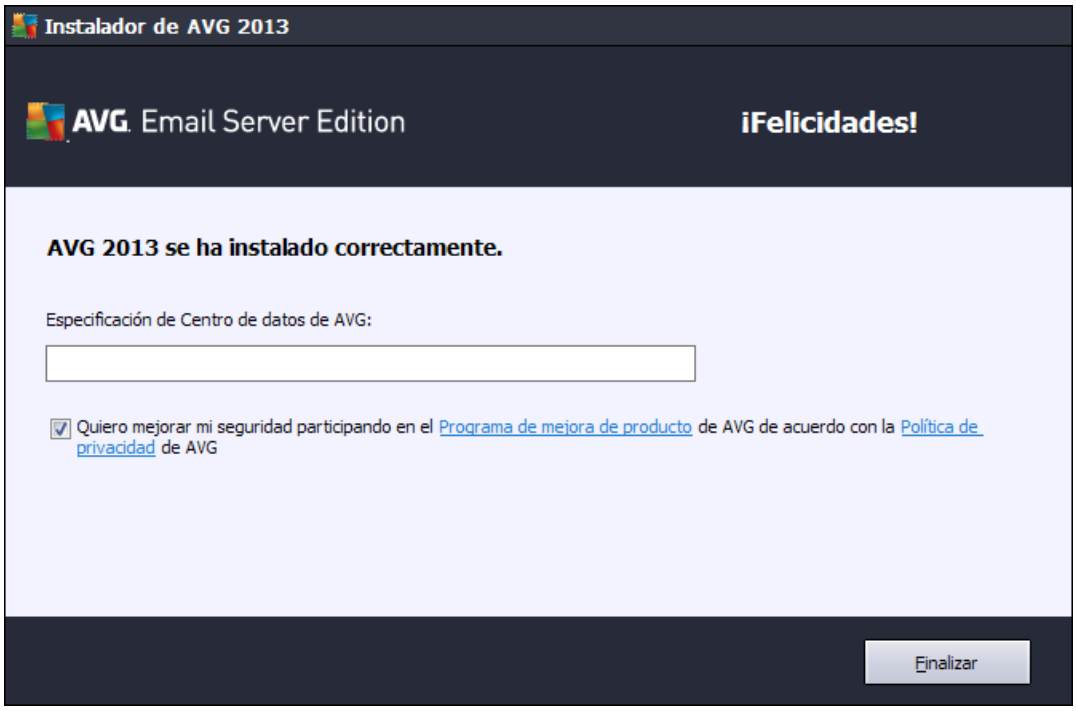
  Comprueba todos los mensajes de correo electrónico almacenados en los buzones de los usuarios. Los virus detectados se mueven al Almacén de virus o se eliminan completamente.

Para los usuarios de Exchange 2003 solo están disponibles los componentes Anti-Spam y Analizador de correo electrónico (VSAPI).

Continúe pulsando el botón ***Siguiente***.

3.6. Finalización de la instalación

Si ha seleccionado el módulo ***Administración remota*** durante la selección de módulos, entonces la pantalla final le permitirá definir la cadena de conexión para conectarse a su Centro de datos de AVG.



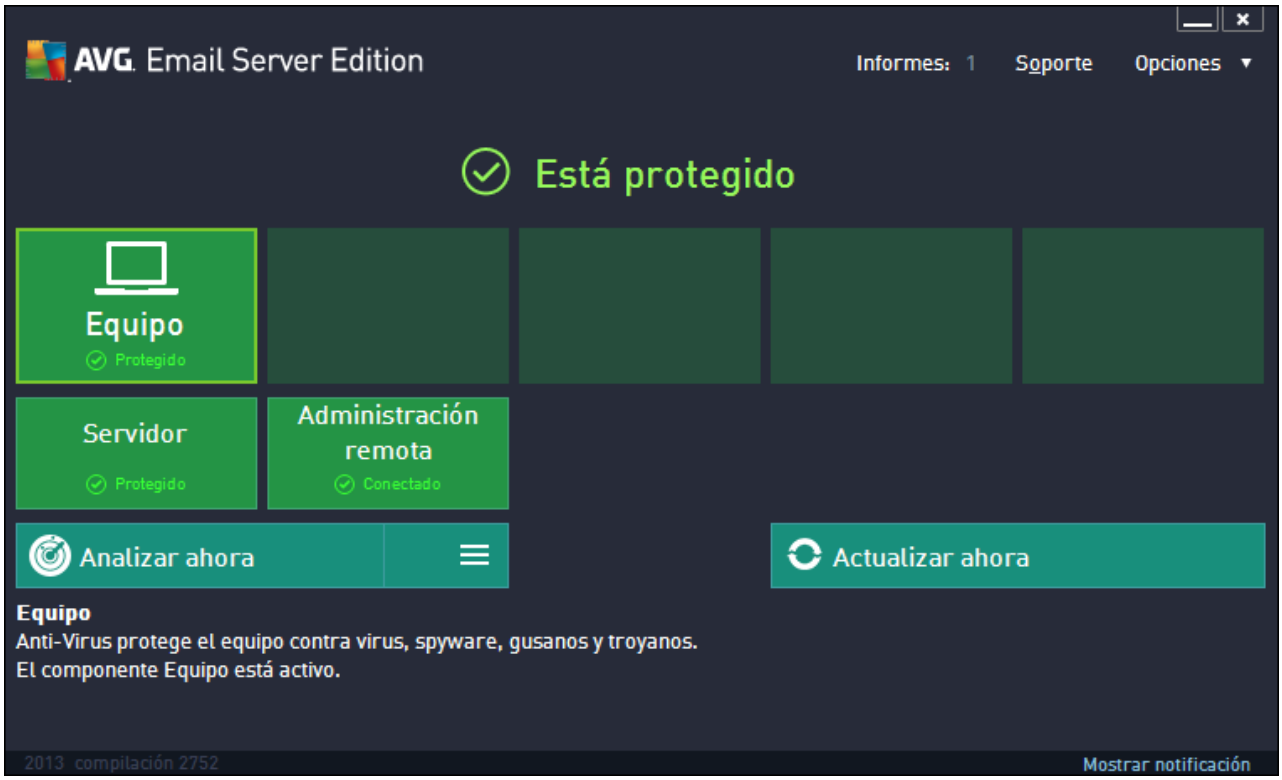
Este cuadro de diálogo también le permite decidir si desea participar en el Programa de mejora de producto, que recopila información anónima sobre las amenazas detectadas para aumentar el nivel de seguridad de Internet. Si acepta esta declaración, mantenga activada la opción ***Quiero mejorar mi seguridad participando en el Programa de mejora de producto de AVG de acuerdo con la Política de privacidad de AVG*** *(la opción está marcada de forma predeterminada)*.

Confirme la selección haciendo clic en el botón **Finalizar**.

Ahora AVG se ha instalado en el equipo y es totalmente funcional. El programa se ejecuta en segundo plano en modo completamente automático.

4. Tras la instalación

Inmediatamente después de que la instalación esté terminada, aparece la pantalla principal de ***AVG Email Server Edition 2013***:



Este manual solo trata las características específicas de ***AVG Email Server Edition 2013***; la configuración y los otros componentes se describen en el manual de AVG Desktop. Para acceder al cuadro de diálogo de los componentes principales del servidor, haga clic en el botón ***Servidor***. Verá la siguiente pantalla:

Tenga en cuenta que todos los componentes del servidor estarán disponibles (excepto si elige no instalar alguno de ellos durante el proceso de instalación) solo si está usando MS Exchange 2007 o superior. MS Exchange 2003 solo admite los componentes AntiSpam y Analizador de correo electrónico (VSAPI).

Para configurar de manera individual la protección para su servidor de correo electrónico, consulte el capítulo correspondiente:

- ***Analizadores de correo electrónico para MS Exchange***
- ***Servidor anti-spam para MS Exchange***
- ***AVG for Kerio MailServer***

5. Analizadores de correo electrónico para MS Exchange

5.1. Información general

Información general básica de los componentes individuales del servidor del analizador de correo electrónico:

- ***EMS (enrutador) - Analizador de correo electrónico para MS Exchange (agente de transporte enrutador)***

  Comprueba todos los mensajes de correo electrónico entrantes, salientes e internos que van a través de la función HUB de MS Exchange.

  Está disponible para MS Exchange 2007/2010/2013 y solo puede instalarse para la función HUB.

- ***EMS (SMTP) - Analizador de correo electrónico para MS Exchange (agente de transporte SMTP)***

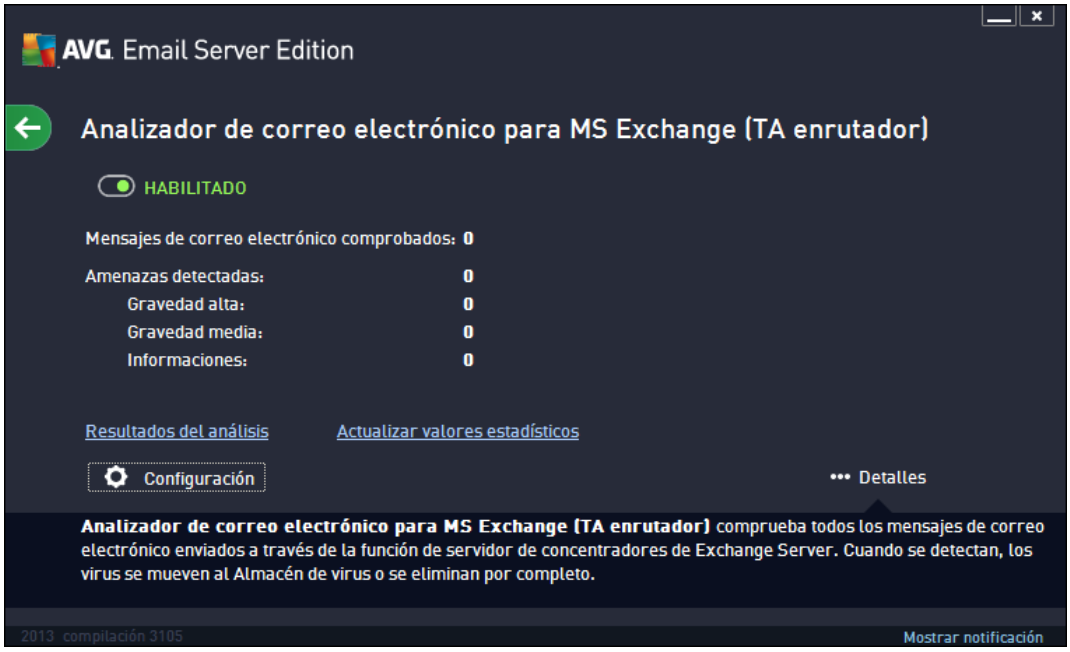
  Comprueba todos los mensajes de correo electrónico que llegan a través de la interfaz SMTP de MS Exchange.

  Solo está disponible para MS Exchange 2007/2010/2013 y puede instalarse tanto para la función HUB como para la EDGE.

- ***EMS (VSAPI) - Analizador de correo electrónico para MS Exchange (VSAPI)***

  Comprueba todos los mensajes de correo electrónico almacenados en los buzones de los usuarios. Los virus detectados se mueven al Almacén de virus o se eliminan completamente.

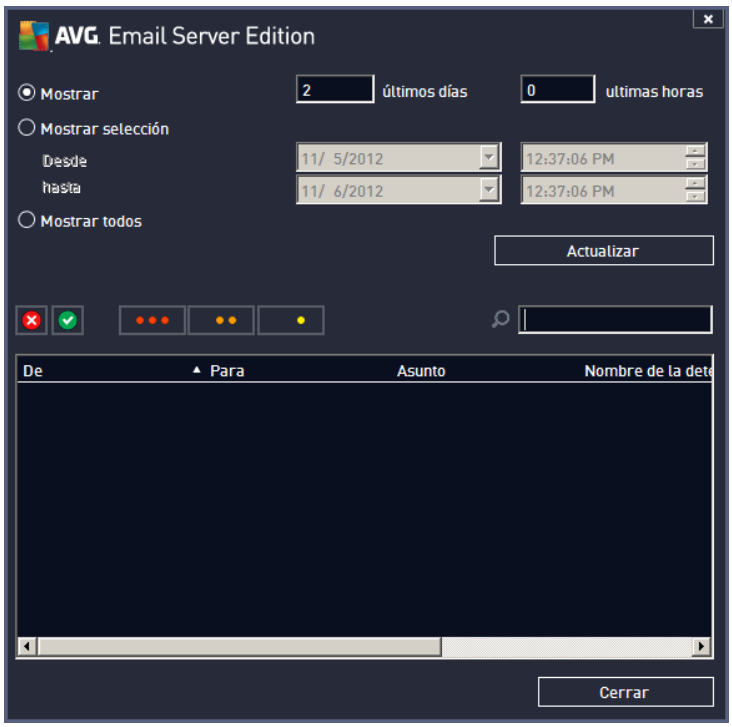
Haga clic en un componente requerido para abrir su interfaz. Todos los componentes comparten los siguientes botones de control y enlaces comunes:



- ***HABILITADO/DESHABILITADO***: al hacer clic en este botón se activa o desactiva el componente seleccionado (si el componente está activado, el botón y el texto son verdes y si está desactivado, son rojos).

- ***Resultados del análisis***

  Abre un nuevo cuadro de diálogo donde puede revisar los resultados del análisis:



  Aquí puede comprobar los mensajes, que aparecen divididos en varias fichas de acuerdo a su gravedad. Consulte la configuración de los componentes individuales para modificar la gravedad y el informe.

  De manera predeterminada, únicamente se muestran los resultados de los últimos dos días. Puede cambiar el período visualizado modificando las opciones siguientes:

  - ***Mostrar últimos***: introduzca los días y horas deseados.
  - ***Mostrar selección***: elija un intervalo de fecha y hora personalizado.
  - ***Mostrar todos***: muestra los resultados para el período completo.

  Utilice el botón ***Actualizar*** para volver a cargar los resultados.

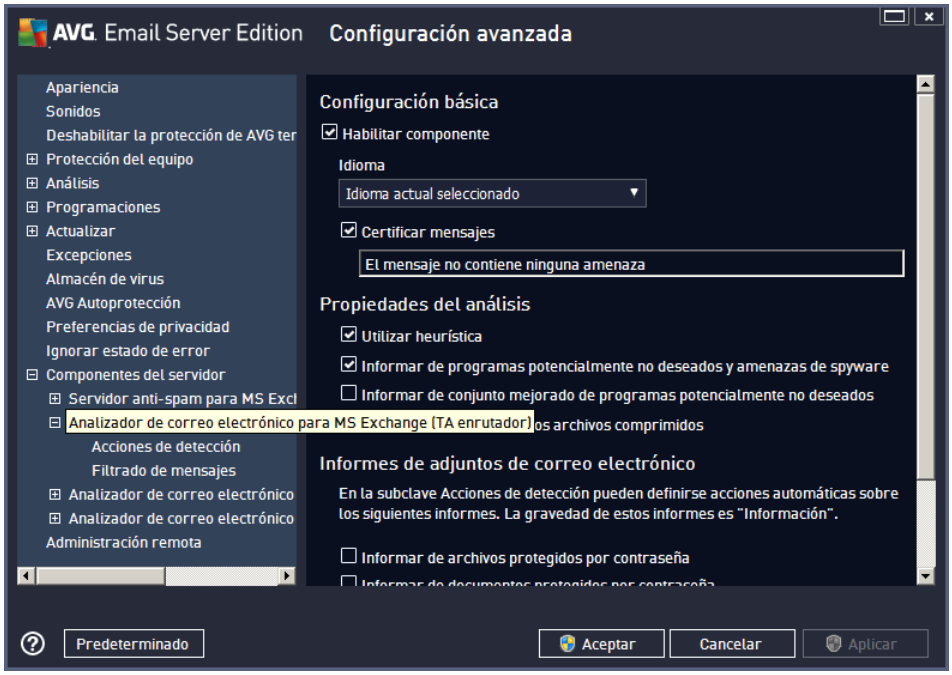
- ***Actualizar valores estadísticos***: actualiza las estadísticas mostradas más arriba.

Al hacer clic en el botón ***Configuración***, se abre la configuración avanzada para el componente seleccionado (encontrará más información sobre la configuración individual de todos los componentes en los siguientes capítulos).

5.2. Analizador de correo electrónico para MS Exchange (TA enrutador)

Para abrir la configuración del ***Analizador de correo electrónico para MS Exchange (agente de transporte enrutador)***, seleccione el botón ***Configuración*** desde la interfaz del componente.

En la lista ***Componentes del servidor*** seleccione el elemento ***Analizador de correo electrónico para MS Exchange (TA enrutador)***:



La sección ***Configuración básica*** ofrece las opciones siguientes:

- ***Habilitar componente***: quite la marca para desactivar todo el componente.
- ***Idioma***: seleccione el idioma deseado del componente.
- ***Certificar mensajes***: marque esta opción si desea añadir una nota de certificación a todos los mensajes analizados. Puede personalizar este mensaje en el siguiente campo.

La sección ***Propiedades del análisis***:

- ***Utilizar heurística***: marque esta casilla para activar el método de detección heurístico durante el análisis.
- ***Informar de programas potencialmente no deseados y amenazas de spyware***: marque esta opción para informar sobre la presencia de programas potencialmente no deseados y spyware.
- ***Informar de conjunto mejorado de programas potencialmente no deseados***: marque esta opción para detectar paquetes ampliados de spyware, es decir, programas perfectamente correctos y que no causan daño alguno cuando se adquieren directamente del fabricante, pero que pueden utilizarse más adelante para fines maliciosos (diversas barras de herramientas, etc.). Se trata de una medida adicional que aumenta aún más la seguridad y la comodidad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada. Nota: esta

característica de detección es adicional a la opción anterior, por lo que si desea protección contra los tipos básicos de spyware, mantenga siempre activa la casilla anterior.

- ***Analizar el contenido de los archivos comprimidos***: marque esta opción para permitir que el analizador busque también en los archivos comprimidos (zip, rar, etc.).

La sección ***Informes de adjuntos de correo electrónico*** le permite seleccionar los elementos de los que se debería informar durante el análisis. Si marca esta opción, cada mensaje de correo electrónico con dicho elemento contendrá la etiqueta [INFORMACIÓN] en el asunto del mensaje. Esta configuración es la predeterminada y puede modificarse fácilmente en la ***sección Acciones de detección***, parte ***Información*** (consulte a continuación).

Las opciones disponibles son las siguientes:

- ***Informar de archivos protegidos por contraseña***
- ***Informar de documentos protegidos por contraseña***
- ***Informar de archivos que contengan macros***
- ***Informar de extensiones ocultas***

Estos subelementos también están disponibles en la siguiente estructura de árbol:

- ***Acciones de detección***
- ***Filtrado de mensajes***

5.3. Analizador de correo electrónico para MS Exchange (TA SMTP)

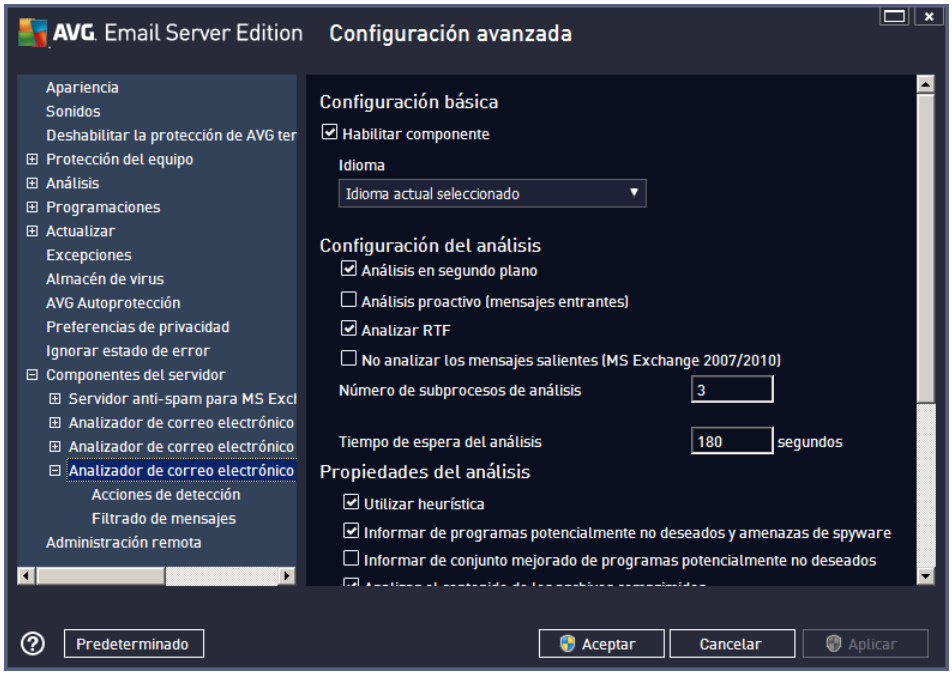
La configuración para el ***Analizador de correo electrónico para MS Exchange (agente de transporte SMTP)*** es exactamente la misma que en el caso del agente de transporte enrutador. Para obtener más información, consulte más arriba el capítulo ***Analizador de correo electrónico para MS Exchange (TA enrutador)***.

Estos subelementos también están disponibles en la siguiente estructura de árbol:

- ***Acciones de detección***
- ***Filtrado de mensajes***

5.4. Analizador de correo electrónico para MS Exchange (VSAPI)

Este elemento contiene la configuración del ***Analizador de correo electrónico para MS Exchange (VSAPI)***.



La sección ***Configuración básica*** ofrece las opciones siguientes:

- ***Habilitar componente***: quite la marca para desactivar todo el componente.
- ***Idioma***: seleccione el idioma deseado del componente.

La sección ***Configuración del análisis***:

- ***Análisis en segundo plano***: aquí puede activar o desactivar el proceso de análisis en segundo plano. El análisis en segundo plano es una de las características de la interfaz de la aplicación VSAPI 2.0/2.5. Ofrece análisis mediante subprocesos para las bases de datos de mensajería de Exchange. Cuando se encuentre en las carpetas de correo del usuario algún elemento que no haya sido analizado con la última actualización de la base de datos de virus de AVG, se enviará a AVG para Exchange Server para que se analice. El análisis y la búsqueda de objetos no examinados se realiza en forma paralela.

  Para cada base de datos se utiliza un subproceso específico de baja prioridad, el cual garantiza que el resto de tareas (por ejemplo, el almacenamiento de mensajes en la base de datos de Microsoft Exchange) siempre tenga preferencia.

- ***Análisis proactivo (mensajes entrantes)***

  Aquí puede activar o desactivar la función de análisis proactivo de VSAPI 2.0/2.5. El análisis ocurre cuando se recibe un elemento en una carpeta sin que el cliente realice ninguna petición.

  En cuanto los mensajes se envían al almacén de Exchange, pasan a estar en la cola del análisis global con baja prioridad (el máximo son 30 elementos). Se analizan según el orden de llegada. Si se accede a un elemento mientras todavía está en la cola, éste cambia a prioridad alta.

Los mensajes de desbordamiento se enviarán al almacén sin analizar.

Aunque desactive las opciones ***Análisis en segundo plano*** y ***Análisis proactivo***, el analizador en acceso estará activo cuando un usuario intente descargar un mensaje con el cliente MS Outlook.

- ***Analizar RTF:*** aquí puede especificar si deberá analizarse o no el tipo de archivo RTF.
- ***No analizar los mensajes salientes (MS Exchange 2007/2010)***: con los componentes de servidor VSAPI y el agente de transporte enrutador (TA enrutador) instalados (independientemente de que sea en un solo servidor o en dos servidores diferentes), puede ocurrir que el correo saliente se analice dos veces. El primer análisis lo realiza el analizador en acceso VSAPI, y el segundo, el agente de transporte enrutador. Esto puede hacer que el servidor vaya más lento y provocar retrasos al enviar correos electrónicos. Si está seguro de que ambos componentes del servidor están instalados y activos, puede evitar este análisis duplicado de los correos electrónicos salientes deshabilitando esta casilla de verificación y el analizador en acceso VSAPI.
- ***Número de subprocesos de análisis:*** de manera predeterminada, el proceso de análisis se realiza mediante subprocesos a fin de aumentar el rendimiento general del análisis al emplear cierto nivel de paralelismo. Aquí puede modificar el número de subprocesos.

  El número predeterminado de subprocesos se computa como 2 veces el 'número de procesadores' + 1.

  El número mínimo de subprocesos se computa como ('número de procesadores'+1) dividido entre 2.

  El número máximo de subprocesos se computa como 'número de procesadores' multiplicado por 5 + 1.

  Si el valor es el mínimo o menor, o el máximo o mayor, se utiliza el valor predeterminado.

- ***Tiempo de espera del análisis***: el intervalo continuo máximo (en segundos) para que un proceso acceda al mensaje que está siendo analizado (el valor predeterminado es de 180 segundos).

La sección ***Propiedades del análisis***:

- ***Utilizar heurística***: marque esta casilla para activar el método de detección heurístico durante el análisis.
- ***Informar de programas potencialmente no deseados y amenazas de spyware***: marque esta opción para informar sobre la presencia de programas potencialmente no deseados y spyware.
- ***Informar de conjunto mejorado de programas potencialmente no deseados***: marque esta opción para detectar paquetes ampliados de spyware, es decir, programas perfectamente correctos y que no causan daño alguno cuando se adquieren directamente del fabricante, pero que pueden utilizarse más adelante para fines maliciosos (diversas barras de herramientas, etc.). Se trata de una medida adicional que aumenta aún más la seguridad y la comodidad del equipo. Sin embargo, puede llegar a bloquear programas genuinos y, por eso, esta opción está desactivada de manera predeterminada. Nota: esta característica de detección es adicional a la opción anterior, por lo que si desea protección contra los tipos básicos de spyware, mantenga siempre activa la casilla anterior.
- ***Analizar el contenido de los archivos comprimidos***: marque esta opción para permitir que el analizador busque también en los archivos comprimidos (zip, rar, etc.).

La sección ***Informes de adjuntos de correo electrónico*** le permite seleccionar los elementos de los que se debería informar durante el análisis. La configuración predeterminada puede modificarse fácilmente en la ***sección Acciones de detección***, parte ***Información*** (consulte a continuación).

Las opciones disponibles son las siguientes:

- ***Informar de archivos protegidos por contraseña***
- ***Informar de documentos protegidos por contraseña***
- ***Informar de archivos que contengan macros***
- ***Informar de extensiones ocultas***

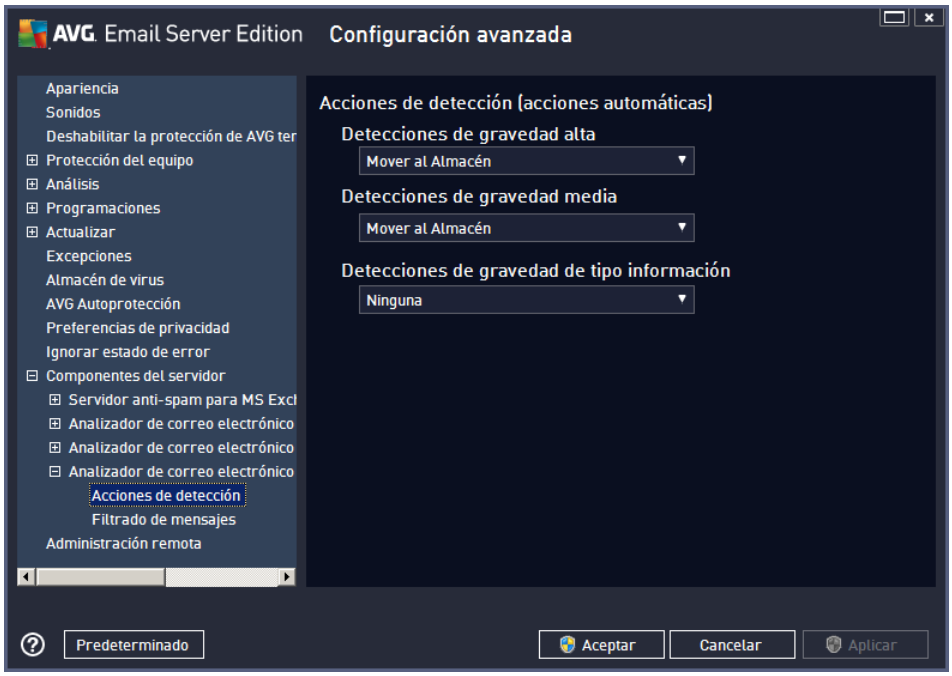
Generalmente, algunas de estas funciones son extensiones del usuario de los servicios de interfaz de la aplicación VSAPI 2.0/2.5 para Microsoft. Para obtener más información sobre VSAPI 2.0/2.5, consulte los siguientes vínculos (y también los vínculos accesibles desde los indicados aquí):

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k: contiene información sobre la interacción entre Exchange y el software antivirus.
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166: contiene información sobre características adicionales de VSAPI 2.5 en la aplicación Exchange 2003 Server.

Estos subelementos también están disponibles en la siguiente estructura de árbol:

- ***Acciones de detección***
- ***Filtrado de mensajes***

5.5. Acciones de detección



En el subelemento ***Acciones de detección*** puede seleccionar las acciones automáticas que deberán llevarse a cabo durante el proceso de análisis.

Las acciones están disponibles para los siguientes elementos:

- ***Detecciones de gravedad alta***: códigos maliciosos que se copian y se propagan por sí solos, a menudo no son percibidos hasta que se produce el daño.
- ***Detecciones de gravedad media***: las consecuencias de tales programas van desde causar daños verdaderamente graves a ser solo posibles amenazas a la privacidad.
- ***Detecciones de gravedad de tipo información***: incluye todas las posibles amenazas detectadas que no pueden clasificarse como ninguna de las categorías antes mencionadas.

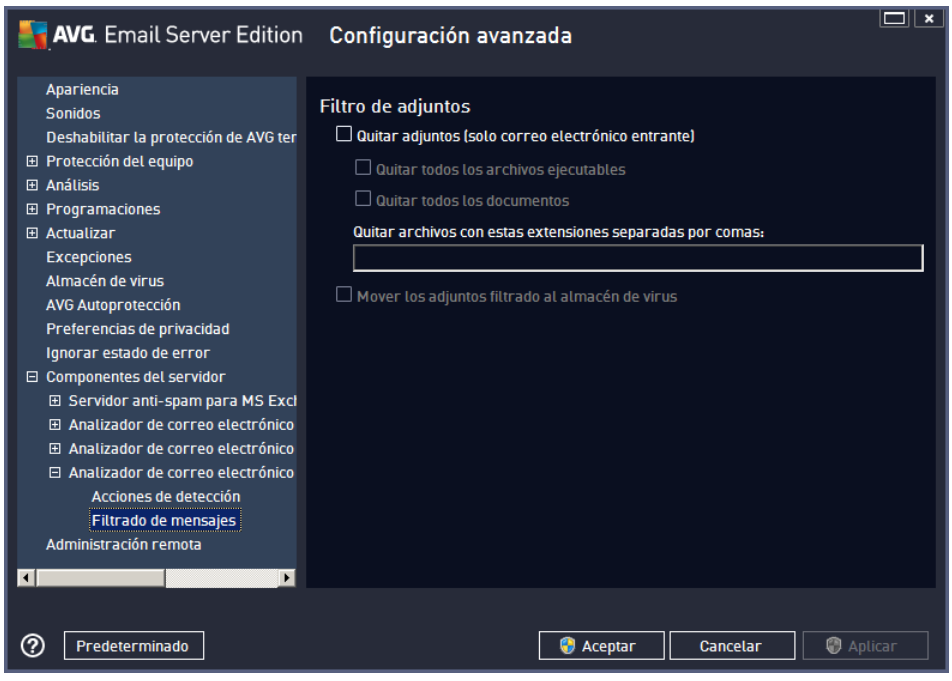
Use el menú desplegable para seleccionar una acción para cada elemento:

- ***Ninguna***: no se llevará a cabo ninguna acción.
- ***Mover al Almacén***: la amenaza en cuestión se enviará al Almacén de virus.
- ***Quitar***: la amenaza en cuestión será eliminada.

Para seleccionar un texto personalizado para el asunto de los mensajes que contengan el elemento o amenaza en cuestión, marque la casilla ***Marcar asunto con...*** e introduzca el valor que desee.

La última característica mencionada no está disponible para el Analizador de correo electrónico para MS Exchange VSAPI.

5.6. Filtrado de mensajes



En el subelemento ***Filtrado de mensajes*** puede elegir los adjuntos que deben eliminarse automáticamente, si hay alguno. Las opciones disponibles son las siguientes:

- ***Quitar adjuntos***: marque esta casilla para habilitar la característica.
- ***Quitar todos los archivos ejecutables***: quita todos los archivos ejecutables.
- ***Quitar todos los documentos***: quita todos los documentos.
- ***Quitar archivos con estas extensiones separadas por comas***: complete la casilla con las extensiones de archivo que desea quitar automáticamente. Separe las extensiones con comas.
- ***Mover los adjuntos filtrados al Almacén de virus***: marque esta opción si no desea que los adjuntos filtrados se eliminen completamente. Si esta casilla de verificación está marcada, todos los adjuntos seleccionados en este cuadro de diálogo se enviarán automáticamente al entorno de cuarentena del Almacén de virus. Éste es un sitio seguro donde almacenar archivos potencialmente peligrosos: aquí puede visualizarlos y examinarlos sin que eso represente un peligro para el sistema. Puede acceder al Almacén de virus desde el menú superior de la interfaz principal de **AVG Email Server Edition 2013**. Simplemente, haga clic con el botón izquierdo en el elemento ***Opciones*** y seleccione el elemento ***Almacén de virus*** en el menú desplegable.

6. Servidor anti-spam para MS Exchange

6.1. Principios de Anti-Spam

El spam se refiere al correo electrónico no solicitado, generalmente anunciando un producto o servicio que se envía masiva y simultáneamente a un gran número de direcciones de correo electrónico, llenando los buzones de los destinatarios. El spam no hace referencia al correo comercial legítimo al que los consumidores dan su consentimiento. El spam no solamente es molesto, sino que también suele ser fuente de estafas, virus o contenidos ofensivos.

Anti-Spam comprueba todos los mensajes entrantes de correo electrónico y marca el correo no deseado como SPAM. Utiliza varios métodos de análisis para procesar cada mensaje, además de ofrecer la máxima protección posible contra el correo no deseado.

6.2. Interfaz de Anti-Spam

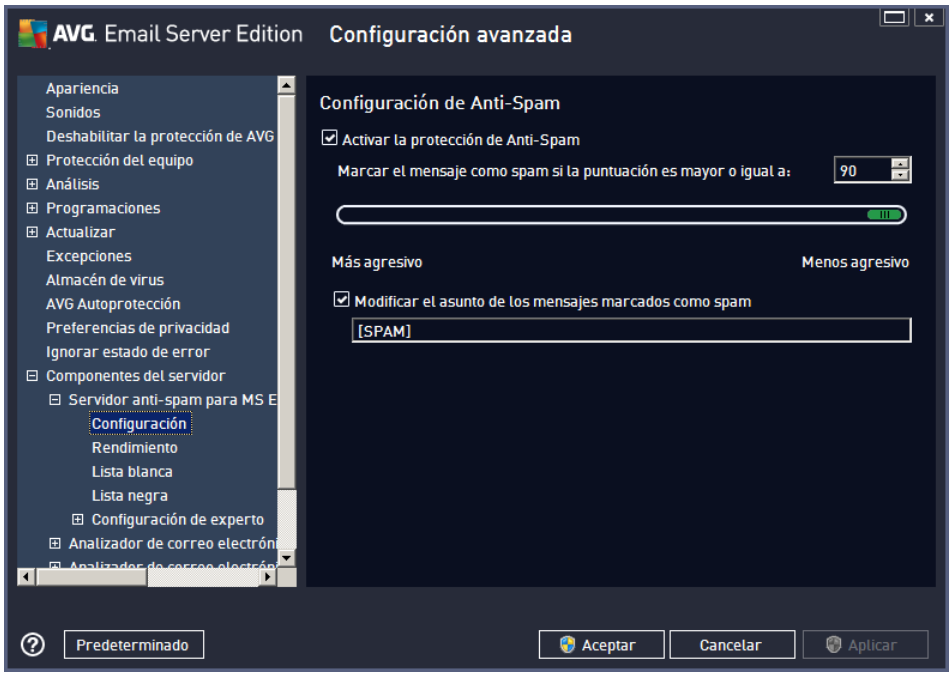
Este cuadro de diálogo contiene información breve sobre la funcionalidad del componente del servidor, su estado actual (*Habilitado/Deshabilitado*) y algunas estadísticas.

Botones y enlaces disponibles:

- ***HABILITADO/DESHABILITADO***: al hacer clic en este botón se activa o desactiva el componente seleccionado (si el componente está activado, el botón y el texto son verdes y si está desactivado, son rojos).
- ***Actualizar valores estadísticos***: actualiza las estadísticas mostradas más arriba.
- ***Configuración***: utilice este botón para abrir la configuración avanzada de Anti-Spam.

6.3. Configuración de Anti-Spam

6.3.1. Configuración



En este cuadro de diálogo, puede marcar la casilla ***Activar la protección de Anti-Spam*** para permitir o impedir el análisis anti-spam de la comunicación por correo electrónico.

En este cuadro de diálogo, también puede seleccionar valores de puntuación más o menos agresivos. El filtro ***Anti-Spam*** asigna una puntuación a cada mensaje (*es decir, el grado de similitud del contenido del mensaje con el spam*) en función de diversas técnicas de análisis dinámico. Puede ajustar la configuración de ***Marcar el mensaje como spam si la puntuación es mayor o igual a*** introduciendo el valor (*50 a 90*) o moviendo el control deslizante a la derecha o izquierda.

A continuación se ofrece un resumen del umbral de puntuación:

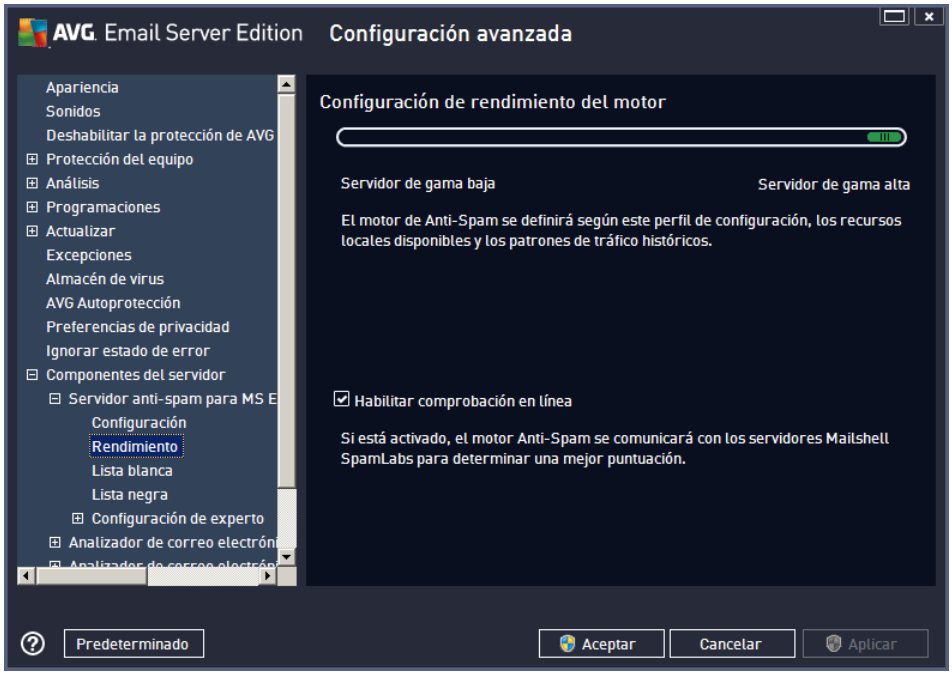
- ***Valor 90***: la mayoría de los mensajes de correo electrónico entrantes se entregarán normalmente (sin ser marcados como spam). El spam más fácilmente identificable se filtrará, pero una cantidad importante de spam se seguirá permitiendo.
- ***Valor 80-89***: los mensajes de correo electrónico con alta probabilidad de ser spam se filtrarán. También pueden filtrarse erróneamente algunos mensajes que no son spam.
- ***Valor 60-79***: considerada como una configuración bastante agresiva. Se filtrarán los mensajes de correo electrónico que posiblemente sean spam. Es probable que también se capturen mensajes que no sean spam.
- ***Valor 50-59***: configuración muy agresiva. Es probable que los mensajes de correo electrónico que no son spam se identifiquen como mensajes de spam auténticos. Este intervalo no se recomienda para uso normal.

Posteriormente puede definir cómo se deben tratar los mensajes de spam detectados:

- ***Modificar el asunto de los mensajes marcados como spam***: marque esta casilla si desea que todos los mensajes detectados como spam estén marcados con una palabra o carácter específico en el asunto del correo; el texto deseado se puede introducir en el campo de texto activo.

- ***Preguntar antes de notificar detección incorrecta***: suponiendo que durante el proceso de instalación aceptara participar en el Programa de mejora de producto (este programa nos ayuda a recopilar información actualizada sobre las amenazas más recientes de parte de personas del mundo entero, lo cual nos permite ofrecer una mejor protección a todos nuestros usuarios), es decir, que aceptara informar a AVG sobre las amenazas detectadas. La notificación se procesa automáticamente. No obstante, puede marcar esta casilla de verificación para confirmar que desea ser consultado antes de informar a AVG sobre spam detectado con el fin de asegurarse de que el mensaje debe clasificarse realmente como spam.

6.3.2. Rendimiento



El cuadro de diálogo ***Configuración de rendimiento del motor*** (*al que se accede mediante el elemento* ***Rendimiento*** *del panel de navegación izquierdo*) ofrece la configuración de rendimiento del componente ***Anti-Spam***. Mueva el control deslizante hacia la izquierda o la derecha para cambiar el nivel de rendimiento del análisis entre los modos ***Poca memoria*** / ***Alto rendimiento***.

- ***Poca memoria***: durante el proceso de análisis realizado para detectar spam, no se utilizarán reglas. Solo se emplearán datos de entrenamiento para la identificación. Este modo no se recomienda para uso común, a menos que el equipo cuente con escasos recursos de hardware.

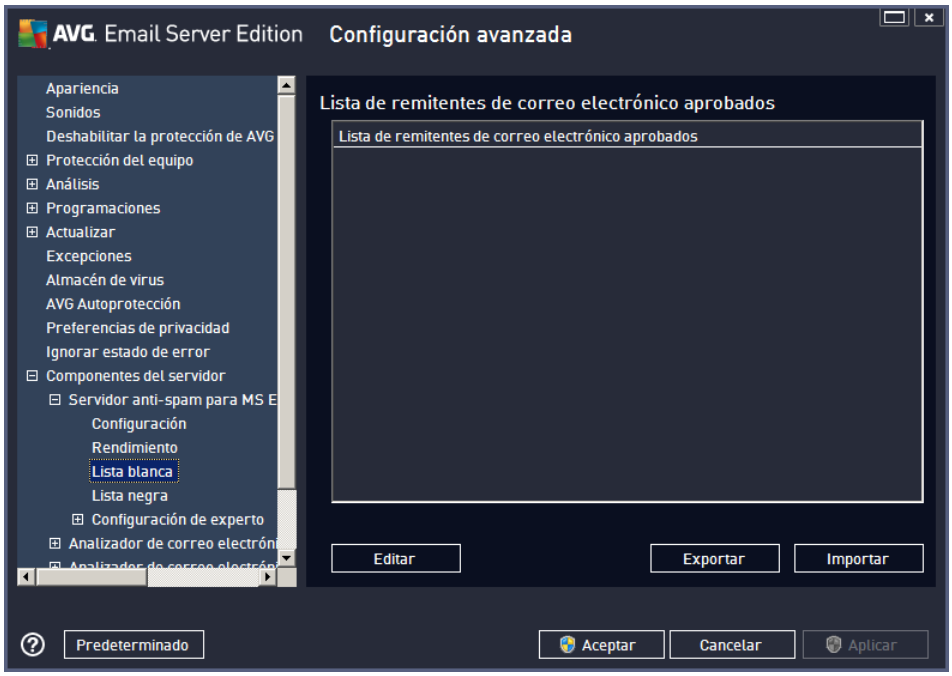
- ***Alto rendimiento***: este modo consumirá una gran cantidad de memoria. Durante el proceso de análisis realizado para detectar spam, se emplearán las siguientes características: reglas y caché de base de datos de spam, reglas básicas y avanzadas, direcciones IP de remitentes que envían spam y bases de datos de remitentes que envían spam.

El elemento ***Habilitar comprobación en línea*** está activado de manera predeterminada. En consecuencia, se obtiene una detección más precisa del spam gracias a la comunicación con los servidores Mailshell; es decir, los datos analizados se compararán con el contenido de la base de datos de Mailshell en línea.

En términos generales, se recomienda mantener la configuración predeterminada y cambiarla únicamente si existe algún motivo que en verdad justifique hacerlo. Cualquier cambio en la configuración solo debe ser realizado por usuarios expertos.

6.3.3. Lista blanca

El elemento ***Lista blanca*** abre un cuadro de diálogo con una lista global de direcciones de correo electrónico y nombres de dominio de remitentes aprobados cuyos mensajes nunca se marcarán como spam.



En la interfaz de edición puede compilar una lista de remitentes de los que tiene la seguridad que nunca le enviarán mensajes no deseados (spam). Del mismo modo, puede compilar una lista de nombres de dominio completos (por ejemplo, *avg.com*), que sabe que no generan mensajes de spam.

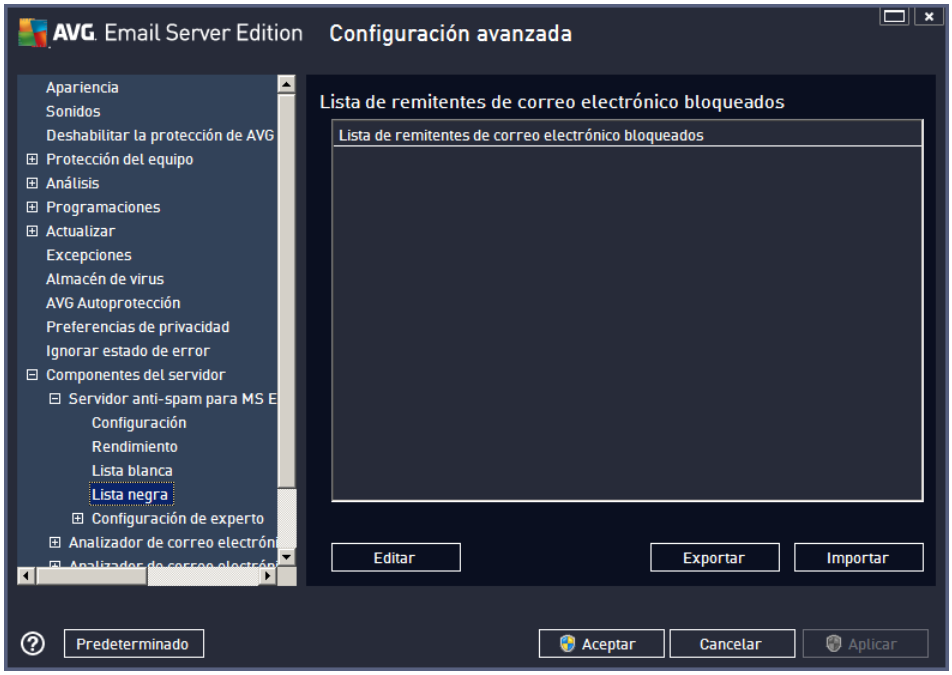
Una vez preparada la lista de remitentes y nombres de dominio, puede introducirlos de dos maneras diferentes: creando una entrada directa de cada dirección de correo electrónico o importando la lista completa de direcciones al mismo tiempo. Los botones de control disponibles son los siguientes:

- ***Editar***: pulse este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (también puede *copiar y pegar*). Inserte un elemento (remitente, nombre de dominio) por línea.
- ***Importar***: puede importar las direcciones de correo electrónico existentes seleccionando este botón. El archivo de entrada puede ser un archivo de texto (en texto sin formato, y el contenido debe tener solo un elemento (dirección o nombre de dominio) por línea) o un archivo WAB, o bien puede realizar la importación desde la libreta de direcciones de Windows o Microsoft Office Outlook.

- ***Exportar***: si por algún motivo decide exportar los registros, puede hacerlo pulsando este botón. Todos los registros se guardarán en un archivo de texto sin formato.

6.3.4. Lista negra

El elemento ***Lista negra*** abre un cuadro de diálogo con una lista global de direcciones de correo electrónico y nombres de dominio de remitentes bloqueados cuyos mensajes se marcarán siempre como spam.



En la interfaz de edición puede compilar una lista de remitentes de los que espera recibir mensajes no deseados (spam). Del mismo modo, puede compilar una lista de nombres de dominio completos (*por ejemplo, empresadespam.com*) de los que espera o recibe mensajes de spam. Todo el correo electrónico procedente de las direcciones o de los dominios enumerados se identificará como spam.

Una vez preparada la lista de remitentes y nombres de dominio, puede introducirlos de dos maneras diferentes: creando una entrada directa de cada dirección de correo electrónico o importando la lista completa de direcciones al mismo tiempo. Los botones de control disponibles son los siguientes:

- ***Editar***: pulse este botón para abrir un cuadro de diálogo donde puede introducir manualmente una lista de direcciones (también puede *copiar y pegar*). Inserte un elemento (remitente, nombre de dominio) por línea.

- ***Importar***: puede importar las direcciones de correo electrónico existentes seleccionando este botón. El archivo de entrada puede ser un archivo de texto (en texto sin formato, y el contenido debe tener solo un elemento (dirección o nombre de dominio) por línea) o un archivo WAB, o bien puede realizar la importación desde la libreta de direcciones de Windows o Microsoft Office Outlook.

- ***Exportar***: si por algún motivo decide exportar los registros, puede hacerlo pulsando este botón. Todos los registros se guardarán en un archivo de texto sin formato.

6.3.5. Configuración de experto

Esta rama contiene numerosas opciones de configuración para el componente Anti-Spam. Estas configuraciones están dirigidas solo a usuarios expertos, administradores de red que necesitan configurar la protección anti-spam con gran detalle para optimizar la seguridad de sus servidores de correo. Por este motivo, no hay ayuda adicional disponible para cada cuadro de diálogo, pero sí se incluye una breve descripción de cada opción directamente en la interfaz de usuario.

Recomendamos encarecidamente no hacer modificaciones en ninguna de las opciones a menos que esté completamente familiarizado con toda la configuración avanzada de Spamcatcher (MailShell Inc.). Cualquier cambio que no sea apropiado puede resultar en un mal rendimiento o en un funcionamiento incorrecto del componente.

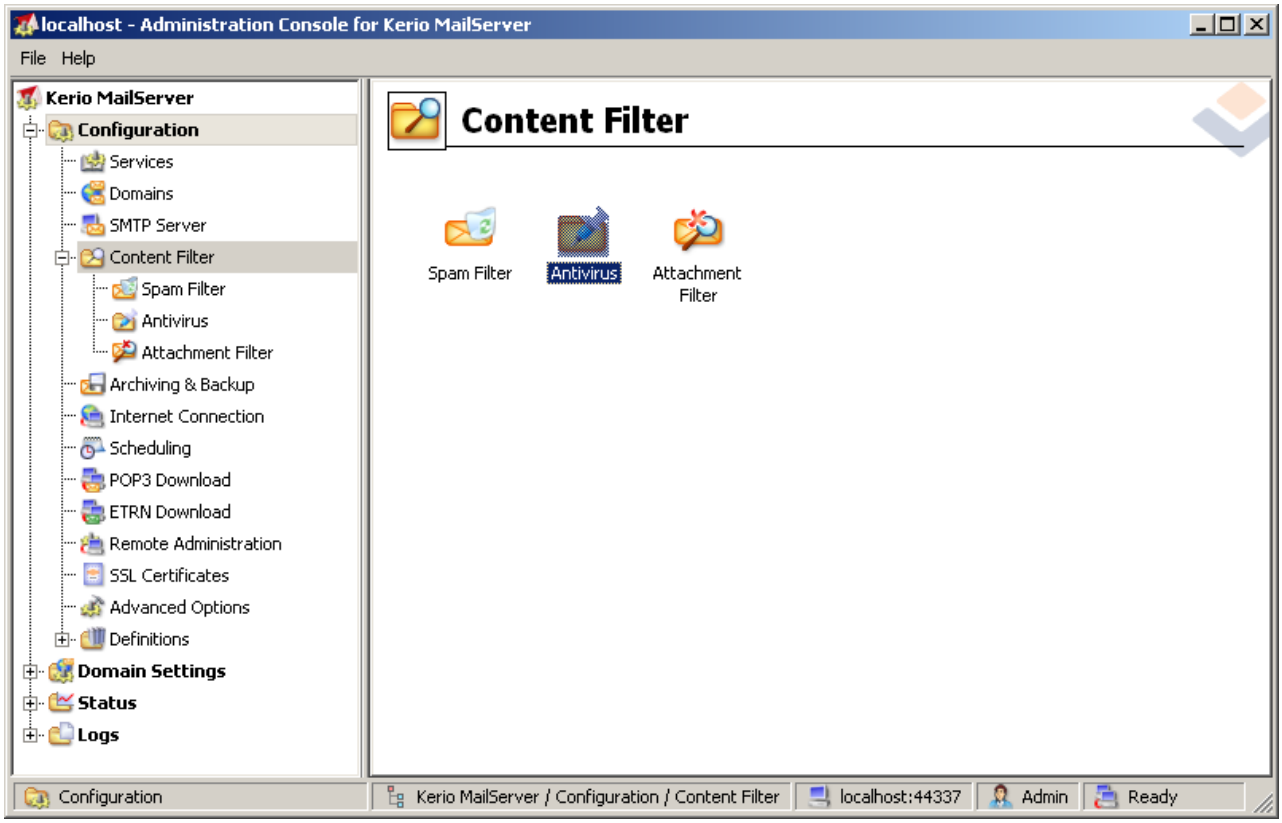
Si aún cree que necesita modificar la configuración de Anti-Spam en el nivel más avanzado, siga las instrucciones proporcionadas directamente en la interfaz de usuario. Por lo general, en cada cuadro de diálogo encontrará una única característica específica que podrá editar y cuya descripción siempre se incluye en el propio cuadro:

- ***Filtrado***: lista de idiomas, lista de países, direcciones IP aprobadas, direcciones IP bloqueadas, países bloqueados, conjuntos de caracteres bloqueados, suplantación de remitentes
- ***RBL***: servidores RBL, múltiples coincidencias, umbral, tiempo de espera, máximo de direcciones IP
- ***Conexión a Internet***: tiempo de espera, servidor proxy, autenticación de proxy

7. AVG for Kerio MailServer

7.1. Configuración

El mecanismo de protección del antivirus está integrado directamente en la aplicación de Kerio MailServer. Para activar la protección para correo electrónico de Kerio MailServer mediante el motor de análisis de AVG, inicie la aplicación Consola de administración de Kerio. En el árbol de control situado a la izquierda de la ventana de la aplicación, seleccione la subrama Filtro de contenido en la rama Configuración:

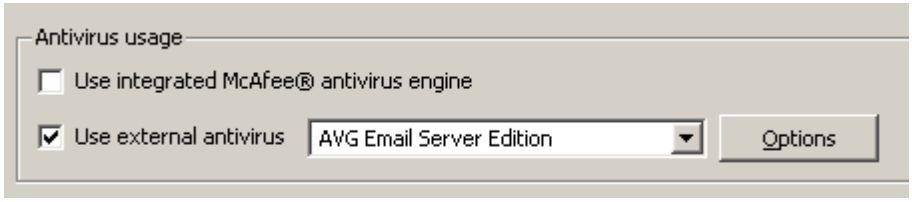


Si hace clic en Filtro de contenido, se mostrará un cuadro de diálogo con tres elementos:

- ***Filtro de spam***
- ***Antivirus*** (consulte la sección ***Antivirus***)
- ***Filtro de archivos adjuntos*** (consulte la sección ***Filtro de archivos adjuntos***)

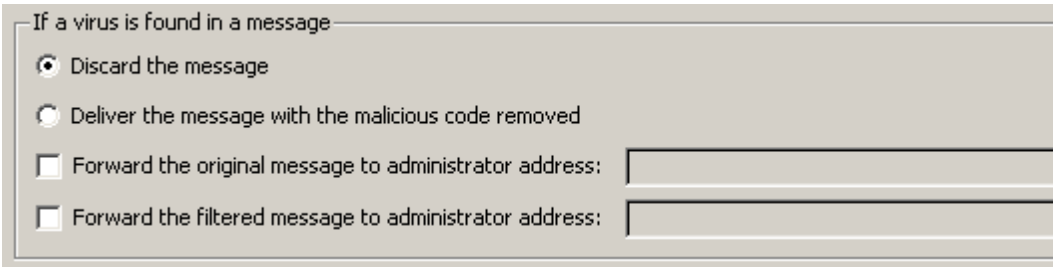
7.1.1. Antivirus

Para activar AVG for Kerio MailServer, seleccione la casilla Utilizar antivirus externo y elija el elemento AVG Email Server Edition en el menú de software externo, en la sección de uso del antivirus de la ventana de configuración:



En la siguiente sección puede especificar lo que desea hacer con un mensaje infectado o filtrado:

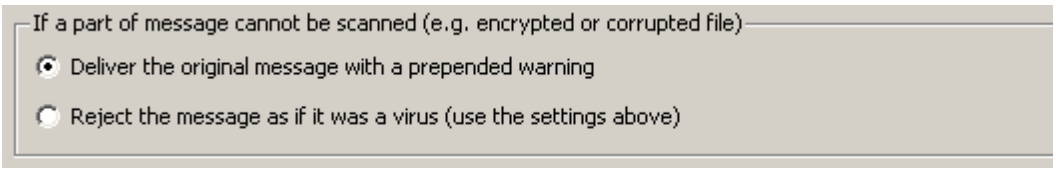
- ***Si se encuentra un virus en un mensaje***



Esta sección especifica la acción que se llevará a cabo cuando se detecte un virus en un mensaje o cuando un filtro de adjuntos filtre un mensaje:

  - ***Descartar mensaje***: si se selecciona, se eliminará el mensaje infectado o filtrado.
  - ***Entregar mensaje después de quitar el código malicioso***: si se selecciona, el mensaje se entregará al receptor, pero sin el adjunto potencialmente dañino.
  - ***Reenviar el mensaje original a la dirección del administrador***: si se selecciona, el mensaje infectado con virus se reenvía a la dirección especificada en el campo de texto de dirección.
  - ***Reenviar el mensaje filtrado a la dirección del administrador***: si se selecciona, el mensaje filtrado se reenvía a la dirección especificada en el campo de texto de dirección.

- ***Si no se puede analizar alguna parte del mensaje (p. ej., un archivo encriptado o dañado)***

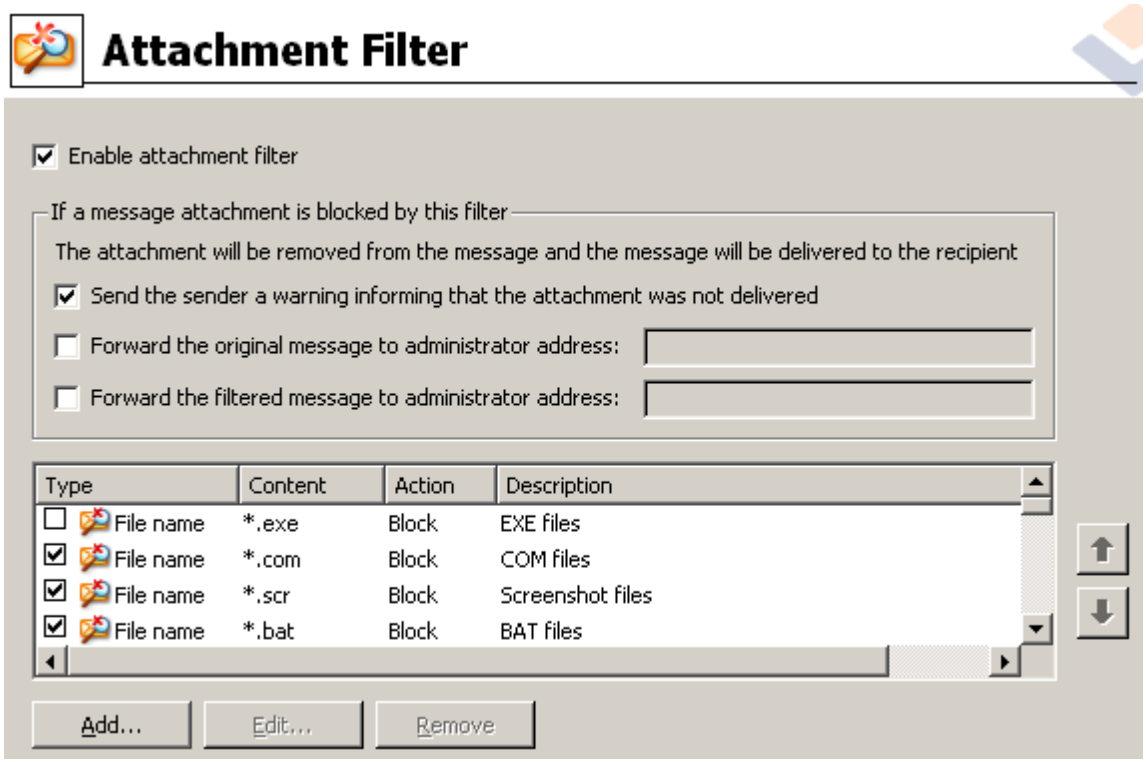


Esta sección especifica la acción que se realizará cuando no se puede analizar parte del mensaje o del archivo adjunto:

  - ***Entregar el mensaje original con un aviso preparado***: el mensaje (o archivo adjunto) se entregará sin comprobar. Se avisará al usuario de que el mensaje podría contener virus.
  - ***Rechazar el mensaje si era un virus***: el sistema reaccionará de la misma forma que cuando se detecta un virus (es decir, el mensaje se entregará sin archivo adjunto o se rechazará). Esta opción es segura, pero será prácticamente imposible enviar archivos protegidos por contraseña.

7.1.2. Filtro de adjuntos

En el menú Filtro de adjuntos, hay una lista de varias definiciones de adjuntos:



Puede habilitar o deshabilitar el filtrado de los adjuntos de correo seleccionando la casilla Habilitar filtro de adjuntos. Puede cambiar la siguiente configuración de forma opcional:

- ***Enviar un aviso al remitente informando de que el adjunto no se ha entregado***

  El remitente recibirá un aviso de Kerio MailServer informándole de que ha enviado un mensaje con un virus o un adjunto bloqueado.

- ***Reenviar el mensaje original a la dirección del administrador***

  El mensaje se reenviará (tal como está, con el adjunto infectado o prohibido) a una dirección de correo electrónico definida, independientemente de que se trate de una dirección local o externa.

- ***Reenviar el mensaje filtrado a la dirección del administrador***

  Se reenviará el mensaje sin el adjunto infectado o prohibido a la dirección de correo especificada (aparte de las acciones seleccionadas más abajo). Esto se puede utilizar para verificar el funcionamiento correcto del antivirus y/o el filtro de adjuntos.

En la lista de extensiones, cada elemento tiene cuatro campos:

- ***Tipo***: especificación del tipo de adjunto, determinado por la extensión dada en el campo Contenido. Tipos posibles son el nombre de archivo o MIME. Puede seleccionar la casilla correspondiente en este campo para incluir o no el elemento en el filtrado de adjuntos.

- ***Contenido***: se puede introducir una extensión para incluirla en el filtrado. Aquí se pueden utilizar caracteres comodín reconocidos por el sistema (por ejemplo, la cadena '*.doc.*' significa cualquier archivo con extensión .doc, y cualquier otra extensión que la siga).

- ***Acción***: defina la acción que se debe realizar con el adjunto específico. Las posibles acciones son Acepto (se acepta el adjunto) y Bloquear (se realizará una acción, según lo que se haya definido sobre la lista de adjuntos deshabilitados).

- ***Descripción***: en este campo se define la descripción del adjunto.

Para quitar un elemento de la lista hay que pulsar el botón Quitar. Puede añadir otro elemento a la lista pulsando el botón ***Agregar...***. O bien puede editar un registro existente pulsando el botón ***Editar...***. A continuación, aparece la siguiente ventana:

- En el campo Descripción puede escribir una descripción corta del adjunto que se debe filtrar.

- En el campo "Si un mensaje contiene un adjunto donde" puede seleccionar el tipo de adjunto (Nombre de archivo o MIME). También puede elegir una extensión en particular de la lista de extensiones ofrecida, o bien escribir directamente el carácter comodín para la extensión.

En el campo "Entonces" puede decidir si desea bloquear el adjunto definido o aceptarlo.

8. Preguntas más frecuentes (FAQ) y soporte técnico

En caso de que tenga algún problema con AVG, ya sea administrativo o técnico, consulte la sección ***Preguntas más frecuentes*** del sitio web de AVG (http://www.avg.com).

Si no consigue encontrar la solución de esta manera, póngase en contacto con el departamento de soporte técnico por correo electrónico. Utilice para ello el formulario de contacto que encontrará en el menú del sistema a través de ***Ayuda / Obtener ayuda en línea***.